Ethical hacking lab: Validation HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

/▲\ Correo /▲\ tiktok /▲\ github

Atacante ---------- |10.10.19.30|

|>/////////// Linux|

Victima ---------- |10.10.11.130|

|> /////// Linux|

| Walkthrough |

Iniciamos el laboratorio comprobando el acceso a la máquina víctima mediante una traza ICMP, la cual revela un TTL característico de un entorno basado en Linux. Procedemos con un escaneo de puertos y servicios utilizando Nmap, encontrando el puerto 22 abierto con SSH en funcionamiento y un servicio web en el puerto 80.

El análisis del servicio web sugiere una vulnerabilidad a una inyección SQL basada en errores. Aprovechamos esta vulnerabilidad para convertirla en una ejecución remota de comandos (RCE) mediante un script en Python, cargando un archivo PHP usando la opción INTOFILE. Esto nos permite invocar funciones de Bash que establecen una shell inversa bajo el usuario www-data.

Luego, localizamos el archivo config.php, que expone una contraseña reutilizada para el usuario root. Con esta información, conseguimos escalar privilegios y obtener acceso completo a la máquina.

| Habilidades |

SQLI (Error Based)

SQL Injection (Error Based): Es un tipo de ataque de inyección SQL donde un atacante explota una vulnerabilidad en una aplicación web para inyectar y ejecutar comandos SQL maliciosos. En este caso, el atacante se basa en los mensajes de error devueltos por la base de datos para obtener información sobre la estructura de la base de datos o para ejecutar comandos SQL arbitrarios. Estos errores pueden revelar detalles como nombres de tablas, columnas y otros datos sensibles.

SQLI -> RCE (INTO OUTFILE)

SQL Injection (SQLI) -> Remote Code Execution (RCE) using INTO OUTFILE: Una vez que un atacante ha identificado una vulnerabilidad de inyección SQL, puede usarla para escribir datos en el sistema de archivos del servidor mediante el uso de la cláusula INTO OUTFILE. Esto permite al atacante cargar archivos, como scripts PHP maliciosos, en el servidor. Estos archivos luego pueden ser ejecutados para obtener una shell inversa o realizar otras acciones, resultando en la ejecución remota de código (RCE).

Information Leakage

Information Leakage: Se refiere a la divulgación no intencionada de información sensible o confidencial. En el contexto de la inyección SQL, la filtración de información puede ocurrir a través de mensajes de error que revelan detalles sobre la estructura de la base de datos, contraseñas, o incluso archivos de configuración que contienen información crítica, como contraseñas de usuario o rutas del sistema.